

IN THE CLAIMS:

1. (Cancelled)

2. (Previously Presented) A contactless IC tag that has a nonvolatile memory and is read and written contactlessly using radio waves, the contactless IC tag being attached to an item which passes through multiple stages of a life cycle from manufacture to disposal, the contactless IC tag comprising:

storing means having stage storage areas as many as the stages of the life cycle;

identifier holding means for holding stage identifiers that each identify a different one of the stage storage areas;

secret receiving means for receiving an access identifier in secrecy from an external access device;

judging means for judging whether the received access identifier matches one of the stage identifiers in the identifier holding means;

access information receiving means for receiving access information from the access device, when the access identifier matches one of the stage identifiers; and

accessing means for accessing a stage storage area that is identified by the access identifier, based on the received access information,

wherein the secret receiving means includes:

authenticator outputting means for generating a first authenticator and outputting the first authenticator to the access device;

20 acquiring means for acquiring a second authenticator that is obtained by
21 encrypting the first authenticator by an encryption algorithm using the access identifier as an
22 encryption key, from the access device; and
23 encrypting means for encrypting the first authenticator by the encryption
24 algorithm using the stage identifiers each as an encryption key, to generate third authenticators,
25 the judging means judges whether the acquired second authenticator matches one
26 of the third authenticators, and if the second authenticator matches one of the third
27 authenticators, judges that the access identifier matches one of the stage identifiers, and
28 the accessing means accesses a stage storage area identified by a stage identifier
29 which is used as an encryption key to generate the third authenticator that matches the second
30 authenticator, as the stage storage area identified by the access identifier.

1 3. (Cancelled)

1 4. (Previously Presented) The contactless IC tag of Claim 2,
2 wherein the authenticator outputting means generates the first authenticator
3 randomly.

1 5. (Original) The contactless IC tag of Claim 4,
2 wherein the secret receiving means further includes:
3 channel selecting means for selecting one of a plurality of communication
4 channels obtained by time-division multiplexing; and
5 identifier receiving means for receiving the access identifier in secrecy, through
6 the selected communication channel.

1 6. (Original) The contactless IC tag of Claim 5,
2 wherein the channel selecting means selects the communication channel
3 randomly.

1 7. (Original) The contactless IC tag of Claim 2,
2 wherein the storing means has a common storage area identified by a common
3 identifier,
4 the identifier holding means stores the common identifier,
5 the judging means judges whether the received access identifier matches the
6 common identifier in the identifier holding means,
7 the access information receiving means receives the access information from the
8 access device, when the access identifier matches the common identifier, and
9 the accessing means accesses the common storage area identified by the access
10 identifier, based on the received access information.

1 8. (Original) The contactless IC tag of Claim 2,
2 wherein the nonvolatile memory is a fuse memory.

1 9. (Original) The contactless IC tag of Claim 2, being provided near a logotype that
2 is positioned on a surface of the item.

1 10. (Original) The contactless IC tag of Claim 2, further comprising
2 time information storing means for storing, when data is stored into the storing
3 means, time information into the storing means together with the data.

1 11. (Original) The contactless IC tag of Claim 2,
2 wherein the storing means has a first memory unit which is non-rewritable and a
3 second memory unit which is rewritable.

1 12. (Original) The contactless IC tag of Claim 2,
2 wherein the storing means has an extension storage area for storing data which
3 cannot be stored in the stage storage areas due to insufficient free space.

1 13. (Original) The contactless IC tag of Claim 10, further comprising
2 memory organizing means for deleting, when data cannot be stored into the
3 storing means due to insufficient free space, data whose time information is oldest from the
4 storing means, to increase the free space.

1 14. (Original) The contactless IC tag of Claim 2, further comprising:
2 master identifier holding means for holding a master identifier;
3 master identifier judging means for judging whether the received access identifier
4 matches the master identifier in the master identifier holding means; and
5 master access information receiving means for receiving master access
6 information from the access device, when the access identifier matches the master identifier,
7 wherein the accessing means accesses one of the stage storage areas based on the
8 received master access information.

1 15-17. (Cancelled)

1 18. (Previously Presented) An access device for sending/receiving information
2 to/from a contactless IC tag that has a nonvolatile memory and is read and written contactlessly
3 using radio waves, the contactless IC tag being attached to an item which passes through
4 multiple stages of a life cycle from manufacture to disposal and having stage storage areas as
5 many as the stages of the life cycle, each stage storage area being identified by a different secret
6 identifier, the access device comprising:

7 identifier storing means for storing an access identifier;

8 secret sending means for sending the access identifier in secrecy to the contactless
9 IC tag; and

10 access information sending means for sending access information to the
11 contactless IC tag, when the contactless IC tag judges that the access identifier properly
12 identifies one of the stage storage areas,

13 wherein the contactless IC tag stores stage identifiers that each identify a different
14 one of the stage storage areas,

15 the secret sending means includes:

16 authenticator receiving means for receiving a first authenticator from the
17 contactless IC tag; and

18 authenticator outputting means for encrypting the received first authenticator by
19 an encryption algorithm using the access identifier as an encryption key to generate a second
20 authenticator, and sending the second authenticator to the contactless IC tag, and

21 the access information sending means sends the access information to the
22 contactless IC tag, when the contactless IC tag (a) encrypts the first authenticator by the

23 encryption algorithm using the stage identifiers each as an encryption key to generate third
24 authenticators, (b) judges whether the second authenticator matches one of the third
25 authenticators, and (c) if the second authenticator matches one of the third authenticators, judges
26 that the access identifier properly identifies one of the stage storage areas.

1 19-25. (Cancelled)

1 26. (New) An information recording medium that is attached to an item which passes
2 through multiple stages of a life cycle from manufacture to disposal, comprising:
3 stage storage areas as many as the stages of the life cycle, each of the stage
4 storage areas storing an encryption key unique to a corresponding stage; and
5 stage identifiers that each identify a different one of the stage storage areas,
6 wherein each of the stage storage areas includes an information storage area that
7 is readable using a first encryption key common to all of the stages, and an information storage
8 area that is readable using a second encryption key unique to a corresponding stage.

1 27. (New) A contactless IC tag that is read and written contactlessly using radio
2 waves, the contactless IC tag being attached to an item which passes through multiple stages of a
3 life cycle from manufacture to disposal, the contactless IC tag comprising:

4 storing means having stage storage areas as many as the stages of the life cycle,
5 each of the stage storage areas including an information storage area that is readable using a first
6 encryption key common to all of the stages and an information storage area that is readable using
7 a second encryption key unique to a corresponding stage;

8 identifier holding means for holding stage identifiers that each identify a different
9 one of the stage storage areas;

10 secret receiving means for receiving an access identifier in secrecy from an
11 external access device;

12 judging means for judging whether the received access identifier matches one of
13 the stage identifiers in the identifier holding means;

14 access information receiving means for receiving access information from the
15 access device, when the access identifier matches one of the stage identifiers; and

16 accessing means for accessing a stage storage area that is identified by the access
17 identifier, based on the received access information.

1 28. (New) The contactless IC tag of Claim 27 having a nonvolatile memory.

2 29. The contactless IC tag of Claim 27,

3 wherein the secret receiving means includes:

4 authenticator outputting means for generating a first authenticator and outputting
5 the first authenticator to the access device;

6 acquiring means for acquiring a second authenticator that is obtained by
7 encrypting the first authenticator by an encryption algorithm using the access identifier as an
8 encryption key, from the access device; and

9 encrypting means for encrypting the first authenticator by the encryption
10 algorithm using the stage identifiers each as an encryption key, to generate third authenticators,

11 the judging means judges whether the acquired second authenticator matches one
12 of the third authenticators, and if the second authenticator matches one of the third
13 authenticators, judges that the access identifier matches one of the stage identifiers, and

14 the accessing means accesses a stage storage area identified by a stage identifier
15 which is used as an encryption key to generate the third authenticator that matches the second
16 authenticator, as the stage storage area identified by the access identifier.

1 30. (New) A contactless IC tag that has a nonvolatile memory and is read and written
2 contactlessly using radio waves, the contactless IC tag being attached to an inpatient who passes
3 through multiple stages of a hospital cycle from admission to release, the contactless IC tag
4 comprising:

5 storing means having stage storage areas as many as the stages of the hospital
6 cycle, each of stage storage areas including an information storage area that is readable using a
7 first encryption key common to all of the stages and an information storage area that is readable
8 using a second encryption key unique to a corresponding stage;

9 identifier holding means for holding stage identifiers that each identify a different
10 one of the stage storage areas;

11 secret receiving means for receiving an access identifier in secrecy from an
12 external access device;

13 judging means for judging whether the received access identifier matches one of
14 the stage identifiers in the identifier holding means;

15 access information receiving means for receiving access information from the
16 access device, when the access identifier matches one of the stage identifiers; and

17 accessing means for accessing a stage storage area that is identified by the access
18 identifier, based on the received access information.

1 31. (New) An access method for use in an access device for sending/receiving
2 information to/from a contactless IC tag that is read and written contactlessly using radio waves,
3 the access device including identifier storing means for storing an access identifier, the
4 contactless IC tag being attached to an item which passes through multiple stages of a life cycle
5 from manufacture to disposal and including storage means which has stage storage areas as many
6 as the stages of the life cycle, each of stage storage areas being identified by a different secret
7 stage identifier and including an information storage area that is readable using a first encryption
8 key common to all of the stages and an information storage area that is readable using a second
9 encryption key unique to a corresponding stage, the access method comprising:

10 a secret sending step for sending the access identifier in secrecy to the contactless
11 IC tag; and

12 an access information sending step for sending access information to the
13 contactless IC tag, when the contactless IC tag judges that the access identifier properly
14 identifies one of the stage storage areas.